

00/60/11
JCS66 U.S. PTOTHE ASSISTANT COMMISSIONER OF PATENTS
Washington, D.C. 20231

11-14-00

DOCKET NUMBER: RPS920000043US1
November 9, 2000

A

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor(s): **Joseph Wayne Freeman, Randall Scott Springfield, Steven Dale Goodman and Isaac Karpel**For: **METHOD TO USE SECURE PASSWORDS IN AN UNSECURE PROGRAM ENVIRONMENT**

Enclosed are:

Patent Specification and Declaration

3 sheets of drawing(s).

An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).

A certified copy of a application.

Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

| For | Number Filed | Number Extra | Rate | Fee |
|---|-----------------|-----------------|---------|------------------------|
| <u>Basic Fee</u> | | | | \$ 710.00 |
| <u>Total Claims</u> | 33 - 20 | 13 | x 18 = | \$ 234.00 |
| <u>Indep. Claims</u> | 6 - 3 | 3 | x 78 = | \$ 234.00 |
| <u>MULTIPLE DEPENDENT CLAIM PRESENTED</u> | | | x 260 = | \$ |
| | | | | TOTAL \$1178.00 |

Please charge IBM Corporation Deposit Account No. 50-0563 in the amount of \$1178.00. A duplicate copy of this sheet is enclosed.

The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 50-0563. A duplicate copy of this sheet is enclosed.

Any additional filing fees required under 37 CFR §1.16.

Any patent application processing fees under 37 CFR §1.17.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" mailing label number: EL139164192US

Date of Mailing: November 9, 2000

I hereby certify that the documents indicated above are being deposited with the United States Postal Service under 37 CFR 1.10 on the date indicated above and are addressed to Box Patent Applications, Assistant Commissioner for Patents, Washington, D.C. 20231 and mailed on the above Date of Mailing with the above "Express Mail" mailing label number.


Beth Costner

Respectfully submitted,

By 
Dan Venglarik
Registration No. 39,409 for
FELSMAN, BRADLEY, VADEN,
GUNTER & DILLON, LLP
201 Main Street, Suite 1600
Fort Worth, Texas 76102
Telephone (817) 332-8143

JC825 U.S. PTO
09/711028

11/09/00

METHOD TO USE SECURE PASSWORDS
IN AN UNSECURE PROGRAM ENVIRONMENT

BACKGROUND OF THE INVENTION

5

1. Technical Field:

The present invention generally relates to data processing system access control and in particular to password controlled access during power up initialization. 10 Still more particularly, the present invention relates to preserving security of a password employed during power up initialization while allowing the password to be employed by the operating system.

10

15 2. Description of the Related Art:

15

Many personal computer systems employ various password schemes to control system behavior before the operating system is started. For example, where a system is used by 20 more than one user, the password may be employed to set "preferences," or user-specific attributes for the operating system behavior.

20

25

30

A potential security problem arises as a result of how the passwords are stored in the system. Particularly on low cost systems, such passwords are commonly stored in a CMOS memory and can be easily read by a program which is run after the operating system is started. Various storage techniques may be employed in storing the passwords to make them less accessible than plain ASCII text strings, such as storing strings of keyboard scan codes or storing a hash of

RPS920000043US1

the ASCII text string or keyboard scan code string.

5 The most secure technique for password storage is to keep the passwords in a nonvolatile storage device which can be locked down "hard" (i.e., requiring a reset to unlock) before the operating system is started. On some systems, several other types of information which is considered sensitive, such as the order of boot device list, is also saved in this lockable storage device.

10

15 Because this technique prevents access to the passwords after the operating system is started, use of the passwords in any other environment other than the "pre-boot" environment is precluded. In some situations, however, use of the passwords to verify the user's identity during operation after the operating system is started may be useful.

20

It would be desirable, therefore, to provide a mechanism for maintaining the security of "pre-boot" passwords while allowing use of such passwords after the operating system is started.

SUMMARY OF THE INVENTION

It is therefore one object of the present invention to provide improved data processing system access control.

5

It is another object of the present invention to provide improved password controlled access during and after power up initialization.

10

It is yet another object of the present invention to provide a mechanism preserving security of a password employed during power up initialization while allowing the password to be employed by the operating system.

15

The foregoing objects are achieved as is now described. During power up initialization, security data such as passwords and other sensitive data which are stored in a lockable memory device are read and copied to protected system management interrupt (SMI) memory space, subject to verification by code running in the SMI memory space that the call to write the security data originates with a trusted entity. Once copied to SMI memory space, the security data is erased from regular system memory and the lockable storage device is hard locked (requiring a reset to unlock) against direct access prior to starting the operating system. The copy of the security data within the SMI memory space is invisible to the operating system.

25

However, the operating system may initiate a call to code running in the SMI memory space to check a password entered by the user, with the SMI code returning a "match" or "no match" indication. The security data may thus be employed after the lockable memory device is hard locked and the

30

RPS920000043US1

operating system is started.

The above as well as additional objectives, features, and advantages of the present invention will become apparent
5 in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a high-level block diagram of a data processing system in which a preferred embodiment of the present invention is implemented;

Figure 2 is a high level flow chart for a process, during power-up initialization, of gathering security data from a nonvolatile storage device and securing that data within the SMI memory space for later use in the operating system environment in accordance with a preferred embodiment of the present invention; and

Figure 3 depicts a high level flow chart for a process of checking the validity of a password required for specific operations to be performed in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures, and in particular with reference to **Figure 1**, a high-level block diagram of a data processing system in which a preferred embodiment of the present invention is implemented is depicted. Data processing system 102 includes a processor 104 coupled via a cache 106 to a system bus 108. Connected to the system bus 108 are various conventional memory devices including a system memory 110, typically a random access memory, and a set of nonvolatile read-only memory (ROM) and/or erasable, electrically programmable read only memory (EEPROM) devices 112. In the present invention, data processing system 102 also includes a "lockable" EEPROM device 114 which may be locked down hard, requiring a reset to unlock, before the operating system is started.

Also attached to system bus 108 are nonvolatile storage 116 such as a hard disk drive and a set of user input/output (I/O) devices 118, which would typically include a keyboard and a mouse or other cursor-control ("pointing") device. Other storage media, such as a CR-ROM or DVD drive, floppy disk drive, and the like may also be employed within data processing system 102, together with other user I/O devices such as a microphone, speakers/headphones, and the like.

The operation of data processing system 102 is well known in the relevant art, and only so much of the operation as is required for an understanding of the present invention

will be described herein. During initial power-on (commonly referred to a "power-on, self-test" or "POST") of data processing system 102, a startup routine including a basic input/output system (BIOS) 120 is loaded from nonvolatile memory devices 112 into system memory 110 and executed to 5 configure the various hardware devices within data processing system 102 for operation by loading device drivers and/or setting system parameters, for instance. An operating system is then loaded from nonvolatile storage 116 and started.

Before the operating system is started, however, the startup routine prompts the user for a password. Once the user enters a password, the startup routine compares the 15 entered password to a password stored within lockable memory device 114. If a match is identified, the operating system is started; if not, either the operating system is not started or the operating system is started without some features enabled. Prior to starting the operating system, however, the lockable memory device 114 is locked down hard 20 to prevent any direct access of the contents by a programming running on the operating system.

In order to allow the password to also be utilized 25 outside the "pre-boot" environment of the startup routine, during the system startup process while the BIOS is still in complete control over data processing system 102, the lockable memory device 114 containing the password(s) and other sensitive data is read out and the content copied to a 30 restricted portion 122 of the system memory 110. This

RPS920000043US1

restricted section 122 of system memory 110 is invisible to the operating system and has associated very tightly defined methods for accessing the contents of restricted memory 122.

5 For Intel-compatible processors, the restricted memory region 122 in the exemplary embodiment 102 is the system management interrupt (SMI) memory space. The SMI memory space contains code and data needed for low level, operating system independent system control functions, and uses a
10 method to authenticate that the calling program which is requesting permission to place data in SMI memory space is a trusted entity (the BIOS startup routine qualifies as such a trusted entity). For other types of processors, a similar restricted memory space which is (1) invisible to the operating system and programs running under the operating system and (2) has access restricted to trusted entities may be employed.

15 After the password(s) and other sensitive data are copied into SMI memory space, the lockable memory device 114 is locked down hard to render the content secure from direct access by programs running under the operating system. Since the password and other sensitive data is still available within the SMI memory space, that information may 20 still be utilized after the operating system boots.

25 Referring to **Figure 2**, a high level flow chart for a process, during power-up initialization, of gathering security data from a nonvolatile storage device and securing 30 that data within the SMI memory space for later use in the operating system environment in accordance with a preferred

embodiment of the present invention is illustrated. The flow chart is drawn to illustrate which steps are performed by the regular POST code and which are performed by code running in the SMI memory space.

5

The process begins as step 202, which depicts the power on reset signal being asserted during power up initialization (POST) as a result of either the application of power to the system (previously powered off) or from a write to a specific input/output device within the system. The power on reset signal resets the hard lock state of the nonvolatile memory device (EEPROM in the exemplary embodiment) containing the passwords and other sensitive data and allows the contents of the EEPROM to be read by the POST BIOS code.

10

15

The process first passes to step 204, which illustrates loading the security data (passwords and other sensitive data) from the EEPROM into regular system memory, and then to step 206, which depicts invoking code present in the SMI memory space with a command which means "Get the security data from regular memory and move that data into SMI memory." The methods of initializing code that runs in SMI space, command calling conventions, and the passing of data pointers are all well known in the art and will not be repeated herein.

20

25

30

Of importance to the next step, when the POST code invokes the code running in SMI space, a label is placed in the source code immediately following the call to invoke the SMI code. When the BIOS is assembled, the address of this label is placed within the SMI code to facilitate the next

step. Only one place within the BIOS code will make this call to the SMI code, enabling the SMI code to ascertain if the call came from the "trusted" caller.

5 The process next passes to step 208, which illustrates determining whether the request is a first request. Only one request to copy data into SMI memory space is allowed for each power-up cycle by limiting the ability to copy data to the SMI memory space to a single request in the exemplary embodiment. Other, similar secure methods may alternatively be employed to restrict copying of data to the SMI memory space. If the request at step 208 is determined not to be a first request, the process proceeds to step 214; if the request is a first request, however, the process passes instead to step 210, which illustrates checking the return address on the stack to determine if the call came from the single trusted routine in the BIOS POST code, and then passes to step 212, which depicts a determination of whether the call came from the trusted routine within the BIOS POST code. If not, the process proceeds to step 214, which illustrates an immediate return to the caller, and doing nothing to the security data area within the SMI memory space. If the call did not come from the trusted BIOS POST routine, the call is essentially ignored, blocking an attack by a program trying to load bogus security data into the SMI memory space.

10 If the call came from the trusted caller within the BIOS POST code, however, the process proceeds instead to step 216, which depicts the code running within the SMI memory space moving the security data from the regular

system memory into the SMI memory space. SMI memory space is invisible to code running from regular system memory, which is the case for any application executing when the operating system is running. The process then passes to 5 step 218, which illustrates the retry counter for attempts to access the security data within SMI memory space being reset.

From either of steps 214 or 218, the process next 10 passes to step 220, which depicts erasing the security data from the regular system memory and sending commands to the EEPROM to "hard lock" the EEPROM against any attempts to read or write the EEPROM (i.e., attempts to read the data in the EEPROM return nothing while attempts to write data to the EEPROM have no effect). This "hard lock" state can only 15 be cleared by the power on reset signal described above in connection with step 202.

The process passes next to step 222, which illustrates 20 running any "untrusted" BIOS extensions and loading the operating system, and then to step 224, which depicts the process becoming idle until the power on reset signal is again asserted.

25 With reference now to **Figure 3**, a high level flow chart for a process of checking the validity of a password required for specific operations to be performed in accordance with a preferred embodiment of the present invention is depicted. Although this example relates 30 specifically to the password, extension of the example shown to other types of security data will be apparent to those

skilled in the art. The process begins at step 302, which depicts an application running under the operating system calling code within the SMI memory space to determine if a password has been set on the system.

5

The process proceeds to step 304, which illustrates the SMI code checking security data within the SMI memory space for the presence of a password and returning a "yes" or "no" response to the calling program indicating whether a password has been set. The process then passes to step 306, which depicts the application running under the operating system determining from the response whether a password is required. If a password has been set, the process proceeds to step 308, which illustrates the application running under the operating system prompting the user for entry of a password string, then calling the SMI code to determine whether the input password string matches the password string stored in the SMI memory space.

10

15

20

25

30

The process then passes to step 310, which depicts incrementing the retry counter (reset in step 216 of Figure 2), and next to step 312, which illustrates a determination of whether the retry counter value exceeds a predetermined maximum number of allowed retries. This step allows only a certain number of retries if the password(s) input by the user do not match the password stored within the SMI memory space, blocking an attack from some code which seeks to discover the password by repeatedly submitting different passwords (e.g., feeding the application executing under the operating system a dictionary) until a match is found.

5 If the retry counter value exceeds the maximum number of allowed retries, the process proceeds to step 314, which depicts returning a "no match" indication to the application running under the operating system. If the retry counter value does not exceed the maximum number of allowed retries however, the process proceeds instead to step 316, which 10 illustrates the SMI code checking the password input by the user against the password stored in the SMI memory space and returning a "match" or "no match" indicator, as appropriate, to the application executing under the operating system.

15 From either of steps 314 or 316, the process passes next to step 318, which illustrates checking the return indication, and then to step 320, which depicts determining whether a "match" indication was returned. If not, the process returns to step 308 to prompt the user to reenter the password. If so, however, the process proceeds instead to step 322, which illustrates the application continuing the task requiring a password until another password is 20 required.

25 One example of how the present invention might be employed is to require password approval for flash memory update operation. In the past, requiring password approval for flash memory updates using the password stored within lockable nonvolatile memory have been impractical under any operating system other than a very basic DOS environment. With the present invention, however, a flash memory update program would call the code within the SMI memory space and 30 ask if a password is required prior to performing a flash memory update operation. If the reply is "yes," the flash

memory update program prompts the user to enter the password. After the password is entered, another call is made to the SMI code to check the validity of the password entered. The SMI code compares the password entered to the data securely stored within the SMI memory space and returns a good/bad indication to the flash memory update program.

The present invention allows the security of passwords stored in memory devices locked prior to starting the operating system to be preserved, while permitting use of the password in a secure manner for applications running under the operating system. Code running within the SMI memory space is employed to verify a password entered, preserving the password security since the password cannot be seen by the operating system.

It is important to note that while the present invention has been described in the context of a fully functional data processing system and/or network, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer usable medium of instructions in a variety of forms, and that the present invention applies equally regardless of the particular type of signal bearing medium used to actually carry out the distribution.

Examples of computer usable mediums include: nonvolatile, hard-coded type mediums such as read only memories (ROMs) or erasable, electrically programmable read only memories (EEPROMs), recordable type mediums such as floppy disks, hard disk drives and CD-ROMs, and transmission type mediums such as digital and analog communication links.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.

CLAIMS:

What is claimed is:

1. A method of enabling use of a secure password,
2 comprising:

3 during power up initialization before an operating
4 system is started, copying security data from a memory
5 device to a restricted portion of system memory which is
6 invisible to the operating system; and

7 before starting the operating system, hard locking the
8 memory device against direct access so that a reset signal
9 is required to unlock the memory device.

1. The method of claim 1, further comprising:

2 responsive to receiving an entered password under the
3 operating system, calling a routine executing within the
4 restricted portion of system memory to verify the password;
5 and

6 receiving an indication from the routine regarding
7 whether the entered password matched a password within the
8 security data copied to the restricted portion of system
9 memory from the memory device.

1. The method of claim 1, wherein the step of copying
2 security data from a memory device to a restricted portion
3 of system memory which is invisible to the operating system
4 further comprises:

5 checking a return address for a call requesting that
6 the security data be copied to verify that the call
7 originated with a trusted routine.

4. The method of claim 3, wherein the step of checking a

2 return address for a call requesting that the security data
3 be copied to verify that the call originated with a trusted
4 routine further comprises:

5 placing a label within a basic input/output services
6 routine implementing a process for copying the security data
7 immediately after instructions for the call requesting that
8 the security data be copied;

9 placing an address for the label within code executing
10 within the restricted portion of system memory and checking
11 the return address for the call requesting that the security
12 data be copied;

13 comparing the return address and the address for the
14 label;

15 responsive to determining that the return address does
16 not match the address for the label, returning a null
17 response to the call requesting that the security data be
18 copied; and

19 responsive to determining that the return address
20 matches the address for the label, copying the security data
21 to the restricted portion of system memory and resetting a
22 retry counter.

1 5. The method of claim 1, wherein the step of copying
2 security data from a memory device to a restricted portion
3 of system memory which is invisible to the operating system
4 further comprises:

5 copying the password and other sensitive data which
6 requires protection from access under the operating system.

1 6. The method of claim 1, wherein the step of copying
2 security data from a memory device to a restricted portion
3 of system memory which is invisible to the operating system

RPS920000043US1

4 further comprises:

5 loading the security data to regular system memory
6 prior to initiating the call requesting that the security
7 data be copied; and

8 upon receiving any response to the call requesting that
9 the security data be copied, erasing the security data from
10 regular system memory before starting the operating system.

1 7. A method of enabling use of a secure password,
2 comprising:

3 responsive to receiving an entered password under an
4 operating system, calling a routine executing within a
5 restricted portion of system memory to verify the password,
6 wherein the restricted portion of system memory is invisible
7 to the operating system and wherein the operating system and
8 routines executing within the restricted portion of system
9 memory communicate through a calling convention; and

10 receiving only an indication from the routine executing
11 within the restricted portion of memory regarding whether
12 the entered password matched a password stored within the
13 restricted portion of system memory.

1 8. The method of claim 7, further comprising:

2 during power up initialization before the operating
3 system is started, copying a password from a memory device
4 to the restricted portion of system memory; and

5 before starting the operating system, hard locking the
6 memory device against direct access so that a reset signal
7 is required to unlock the memory device.

1 9. The method of claim 7, further comprising:

2 determining whether a password is required for an
3 operation by checking with the routine executing within a
4 restricted portion of system memory to verify existence of a
5 password.

1 10. The method of claim 7, further comprising:

2 limiting a number of retries for a user to reenter a
3 password.

RPS920000043US1

1 11. The method of claim 7, further comprising:

2 transmitting the entered password entered by a user to
3 the routine executing within a restricted portion of system
4 memory using the calling convention; and

5 responsive to receiving an indication from the routine
6 executing within the restricted portion of memory that the
7 entered password matched the password stored within the
8 restricted portion of system memory, continuing an operation
9 requiring the entered password for execution.

1 12. A data processing system, comprising:

2 a memory device which may be hard locked against direct
3 access so that a reset signal is required to unlock the
4 memory device; and

5 a power up initialization routine executing within the
6 data processing system,

7 wherein the power up initialization routine, before
8 starting an operating system, copies security data from the
9 memory device to a restricted portion of system memory which
10 is invisible to the operating system and hard locks the
11 memory device.

1 13. The data processing system of claim 12, wherein the
2 power up initialization routine, responsive to receiving an
3 entered password under the operating system, calls a routine
4 executing within the restricted portion of system memory to
5 verify the password and receives an indication from the
6 routine regarding whether the entered password matched a
7 password within the security data copied to the restricted
8 portion of system memory from the memory device.

1 14. The data processing system of claim 13, wherein the
2 routine executing within the restricted portion of system
3 memory checks a return address for a call requesting that
4 the security data be copied to verify that the call
5 originated with a trusted routine.

1 15. The data processing system of claim 13, wherein the
2 power up initialization routine, to facilitate checking a
3 return address for a call requesting that the security data
4 be copied to verify that the call originated with a trusted
5 routine, places a label within a basic input/output services

6 routine implementing a process for copying the security data
7 immediately after instructions for the call requesting that
8 the security data be copied,

9 wherein the routine executing within the restricted
10 portion of system memory contains an address for the label,
11 checks the return address for the call requesting that the
12 security data be copied, and compares the return address and
13 the address for the label and,

14 responsive to determining that the return address
15 does not match the address for the label, returning a
16 null response to the call requesting that the security
17 data be copied, and

18 responsive to determining that the return address
19 matches the address for the label, copying the security
20 data to the restricted portion of system memory and
21 resetting a retry counter.

1 16. The data processing system of claim 12, wherein the
2 power up initialization routine copies the password and
3 other sensitive data which requires protection from access
4 under the operating system.

1 17. The data processing system of claim 12, wherein the
2 power up initialization routine loads the security data to
3 regular system memory prior to initiating the call
4 requesting that the security data be copied and, upon
5 receiving any response to the call requesting that the
6 security data be copied, erases the security data from
7 regular system memory before starting the operating system.

1 18. A data processing system, comprising:
2 an operating system;
3 a memory device which may be hard locked against direct
4 access so that a reset signal is required to unlock the
5 memory device;

6 a system memory including a restricted portion
7 invisible to the operating system, wherein the operating
8 system and routines executing within the restricted portion
9 of system memory communicate through a calling convention;
10 and

11 a power up initialization routine executing within the
12 data processing system, wherein the power up initialization
13 routine, responsive to receiving an entered password under
14 an operating system, calls a routine executing within a
15 restricted portion of system memory to verify the password,
16 and receives only an indication from the routine executing
17 within the restricted portion of memory regarding whether
18 the entered password matched a password stored within the
19 restricted portion of system memory.

1 19. The data processing system of claim 18, wherein the
2 power up initialization routine, during power up
3 initialization before the operating system is started,
4 copies a password from the memory device to the restricted
5 portion of system memory and, before starting the operating
6 system, hard locks the memory device against direct access
7 so that a reset signal is required to unlock the memory
8 device.

1 20. The data processing system of claim 18, wherein the
2 power up initialization routine determines whether a
3 password is required for an operation by checking with the

4 routine executing within a restricted portion of system
5 memory to verify existence of a password.

1 21. The data processing system of claim 18, wherein the
2 routine executing within a restricted portion of system
3 memory to verify the password limits a number of retries for
4 a user to reenter a password.

1 22. The data processing system of claim 18, wherein the
2 power up initialization routine transmits the entered
3 password entered by a user to the routine executing within a
4 restricted portion of system memory using the calling
5 convention and, responsive to receiving an indication from
6 the routine executing within the restricted portion of
7 memory that the entered password matched the password stored
8 within the restricted portion of system memory, continues an
9 operation requiring the entered password for execution.

1 23. A computer program product within a computer usable
2 medium for enabling use of a secure password, comprising:
3 instructions for copying security data from a memory
4 device to a restricted portion of system memory which is
5 invisible to the operating system during power up
6 initialization before an operating system is started; and
7 instructions for hard locking the memory device against
8 direct access so that a reset signal is required to unlock
9 the memory device before starting the operating system.

1 24. The computer program product of claim 23, further
2 comprising:

3 instructions, responsive to receiving an entered
4 password under the operating system, for calling a routine
5 executing within the restricted portion of system memory to
6 verify the password; and

7 instructions for receiving an indication from the
8 routine regarding whether the entered password matched a
9 password within the security data copied to the restricted
10 portion of system memory from the memory device.

1 25. The computer program product of claim 23, wherein the
2 instructions for copying security data from a memory device
3 to a restricted portion of system memory which is invisible
4 to the operating system further comprise:

5 instructions for checking a return address for a call
6 requesting that the security data be copied to verify that
7 the call originated with a trusted routine.

1 26. The computer program product of claim 25, wherein the
2 instructions for checking a return address for a call
3 requesting that the security data be copied to verify that

4 the call originated with a trusted routine further comprise:

5 instructions for placing a label within a basic
6 input/output services routine implementing a process for
7 copying the security data immediately after instructions for
8 the call requesting that the security data be copied;

9 an address for the label within code executing within
10 the restricted portion of system memory and checking the
11 return address for the call requesting that the security
12 data be copied;

13 instructions for comparing the return address and the
14 address for the label;

15 instructions, responsive to determining that the return
16 address does not match the address for the label, for
17 returning a null response to the call requesting that the
18 security data be copied; and

19 instructions, responsive to determining that the return
20 address matches the address for the label, for copying the
21 security data to the restricted portion of system memory and
22 resetting a retry counter.

1 27. The computer program product of claim 23, wherein the
2 instructions for copying security data from a memory device
3 to a restricted portion of system memory which is invisible
4 to the operating system further comprise:

5 instructions for copying the password and other
6 sensitive data which requires protection from access under
7 the operating system.

1 28. The computer program product of claim 23, wherein the
2 instructions for copying security data from a memory device
3 to a restricted portion of system memory which is invisible
4 to the operating system further comprise:

RPS920000043US1

5 instructions for loading the security data to regular
6 system memory prior to initiating the call requesting that
7 the security data be copied; and

8 instructions for erasing the security data from regular
9 system memory before starting the operating system upon
10 receiving any response to the call requesting that the
11 security data be copied.

1 29. A computer program product within a computer usable
2 medium for enabling use of a secure password, comprising:
3 instructions, responsive to receiving an entered
4 password under an operating system, for calling a routine
5 executing within a restricted portion of system memory to
6 verify the password, wherein the restricted portion of
7 system memory is invisible to the operating system and
8 wherein the operating system and routines executing within
9 the restricted portion of system memory communicate through
10 a calling convention; and

11 instructions for receiving only an indication from the
12 routine executing within the restricted portion of memory
13 regarding whether the entered password matched a password
14 stored within the restricted portion of system memory.

1 30. The computer program product of claim 29, further
2 comprising:

3 instructions for copying a password from a memory
4 device to the restricted portion of system memory during
5 power up initialization before the operating system is
6 started; and

7 instructions for hard locking the memory device against
8 direct access so that a reset signal is required to unlock
9 the memory device before starting the operating system.

1 31. The computer program product of claim 29, further
2 comprising:

3 instructions for determining whether a password is
4 required for an operation by checking with the routine
5 executing within a restricted portion of system memory to
6 verify existence of a password.

RPS920000043US1

1 32. The computer program product of claim 29, further
2 comprising:

3 instructions for limiting a number of retries for a
4 user to reenter a password.

1 33. The computer program product of claim 29, further
2 comprising:

3 instructions for transmitting the entered password
4 entered by a user to the routine executing within a
5 restricted portion of system memory using the calling
6 convention; and

7 instructions, responsive to receiving an indication
8 from the routine executing within the restricted portion of
9 memory that the entered password matched the password stored
10 within the restricted portion of system memory, for
11 continuing an operation requiring the entered password for
12 execution.

METHOD TO USE SECURE PASSWORDS
IN AN UNSECURE PROGRAM ENVIRONMENT

ABSTRACT OF THE DISCLOSURE

5

During power up initialization, security data such as
passwords and other sensitive data which are stored in a
lockable memory device are read and copied to protected
system management interrupt (SMI) memory space, subject to
verification by code running in the SMI memory space that
the call to write the security data originates with a
trusted entity. Once copied to SMI memory space, the
security data is erased from regular system memory and the
lockable storage device is hard locked (requiring a reset to
unlock) against direct access prior to starting the
operating system. The copy of the security data within the
SMI memory space is invisible to the operating system.
However, the operating system may initiate a call to code
running in the SMI memory space to check a password entered
by the user, with the SMI code returning a "match" or "no
match" indication. The security data may thus be employed
after the lockable memory device is hard locked and the
operating system is started.

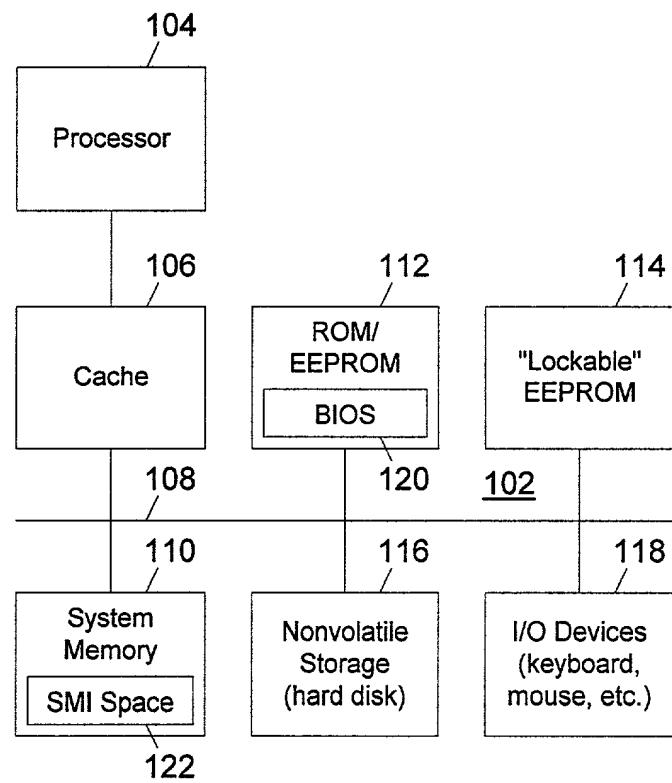


Figure 1

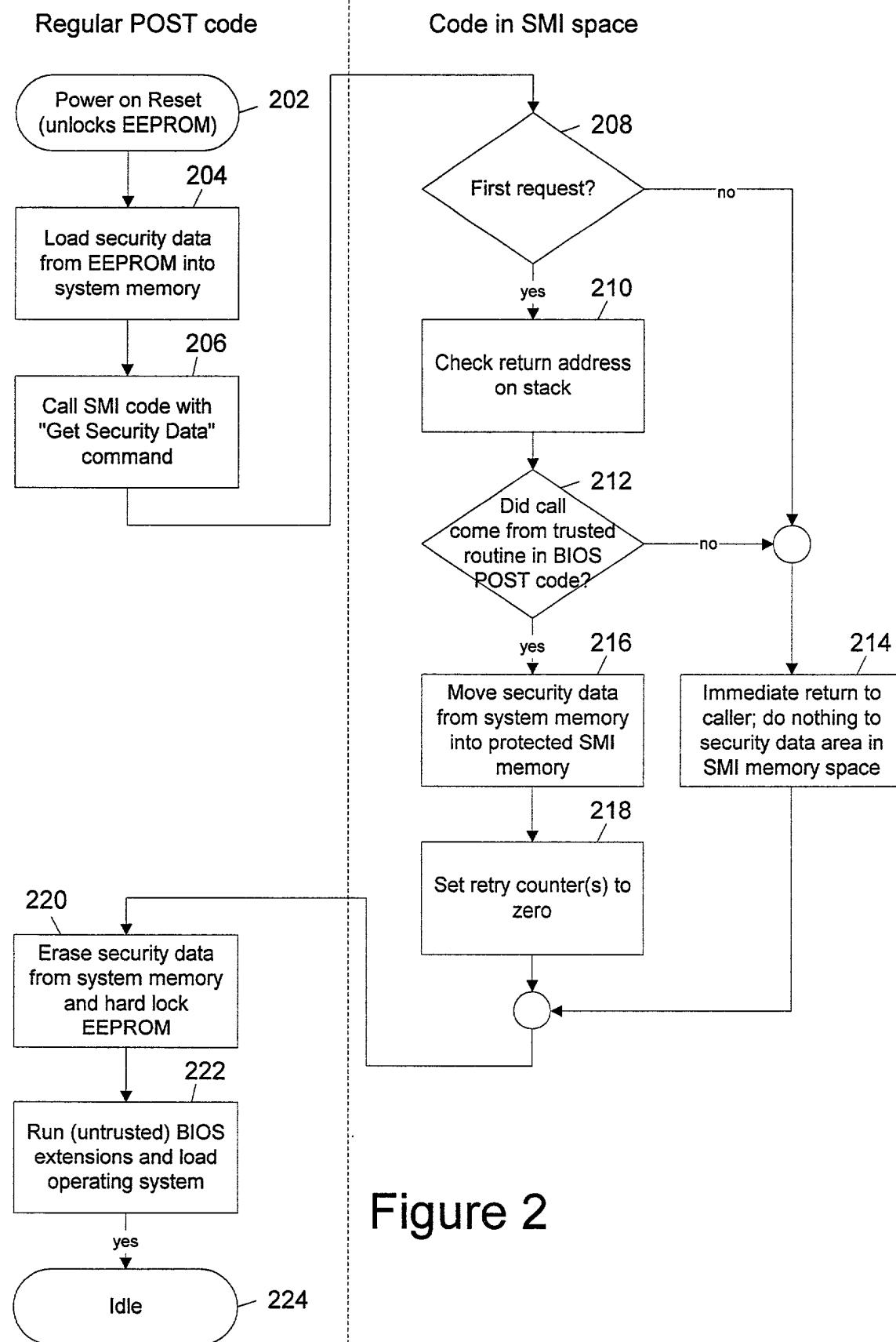


Figure 2

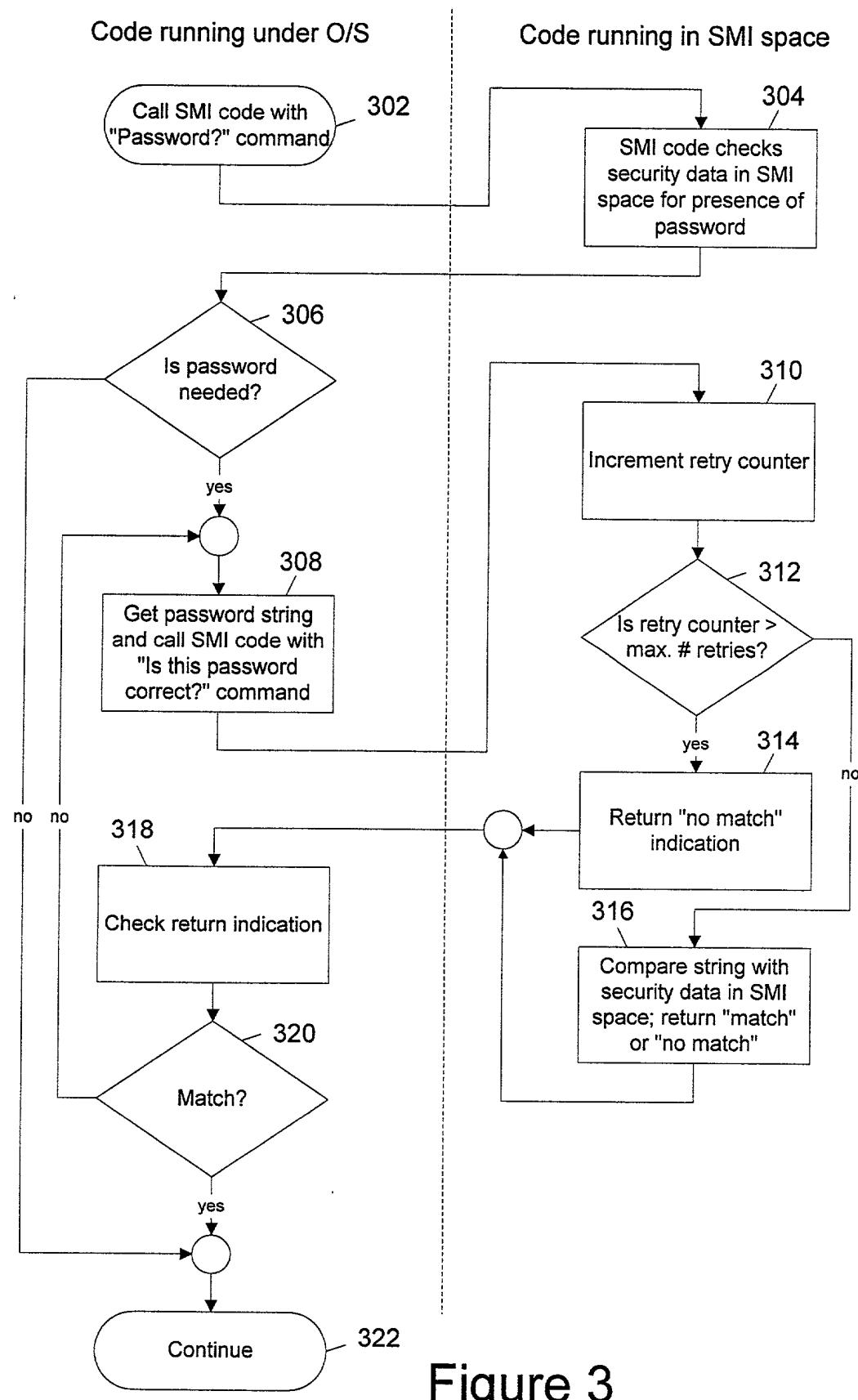


Figure 3

DOCKET NUMBER: RES920000043US1DECLARATION AND POWER OF ATTORNEY FOR
PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD TO USE SECURE PASSWORDS IN AN UNSECURE PROGRAM ENVIRONMENT

the specification of which (check one)

is attached hereto.

was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

Priority Claimed

| (Number) | (Country) | (Day/Month/Year) | Yes | No |
|----------|-----------|------------------|-----|----|
|----------|-----------|------------------|-----|----|

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| (Application Serial #) | (Filing Date) | (Status) |
|------------------------|---------------|----------|
|------------------------|---------------|----------|

JC625 U.S. PTO
09/11/028

11/09/00

DOCKET NUMBER: RPS920000043US1

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Horace St. Julian, Reg. No. 30,329; J. Bruce Schelkopf, Reg. No. 43,901; John D. Flynn, Reg. No. 35,137; George E. Grosser, Reg. No. 25,629; Martin J. McKinley, Reg. No. 31,782; Christopher A. Hughes, Reg. No. 26,914; John E. Noel, Reg. No. 26,275; Joseph C. Redmond, Jr., Reg. No. 18,753; Andrew J. Dillon, Reg. No. 29,634; Daniel N. Venglarik, Reg. No. 39,409; Jack V. Musgrave, Reg. No. 31,986; Brian P. Russell, Reg. No. 40,796; Matthew W. Baca, Reg. No. 42,277; Antony P. Ng, Reg. No. 43,427; John G. Graham, Reg. No. 19,563; Michael R. Baxce, Reg. No. 44,023; Richard N. McCain, Reg. No. 43,785 and Michael E. Now, Reg. No. 44,975.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Lakewood on the Park, Suite 350, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, 512/343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: Joseph Wayne Freeman

INVENTORS SIGNATURE: Joseph Wayne Freeman DATE: Nov. 9, 2000

RESIDENCE: 5820 Glenfiddich Way
Raleigh, North Carolina 27613

CITIZENSHIP: United States of America

POST OFFICE ADDRESS: same

FULL NAME OF SOLE OR SECOND INVENTOR: Randall Scott Springfield

INVENTORS SIGNATURE: Randall Scott Springfield DATE: 11/9/2000

RESIDENCE: 107 Garden Gate Drive
Chapel Hill, North Carolina 27516

CITIZENSHIP: United States of America

POST OFFICE ADDRESS: same

DOCKET NUMBER: RPS920000043US1

FULL NAME OF SOLE OF THIRD INVENTOR: Steven Dale Goodman

INVENTORS SIGNATURE: Steven Dale Goodman DATE: November 9, 2000

RESIDENCE: 5153 Jeffries Street
Raleigh, North Carolina 27606

CITIZENSHIP: United States of America

POST OFFICE ADDRESS: same

FULL NAME OF SOLE OF FOURTH INVENTOR: Isaac Karpel

INVENTORS SIGNATURE: Isaac Karpel DATE: 11/09/00

RESIDENCE: 106 Ashley Brook Court
Cary, North Carolina 27513

CITIZENSHIP: United States of America

POST OFFICE ADDRESS: same